Policy Document Control Page

Title

Title: Data Protection Policy

Version: 4

Reference Number: CO59

Keywords:
Data, access, principles, protection, Act. Data Subject, Information

Supersedes
Supersedes: Version 3
Description of Amendment(s):

- **Policy amended to include responsibilities and further guidance regarding the Data Protection Principles.**

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Information Governance Manager
ERA undertaken on: 31.10.2011
ERA approved by EIA Work group on: 08.11.2011

Where policy deemed relevant to equality-
EIA undertaken by Information Governance Manager
EIA undertaken on 31.10.2011
EIA approved by EIA work group on 08.11.2011

Approval and Ratification

Referred for approval by: Information Governance Manager

Date of Referral: February 2016

Approved by: Virtual IAOs / IGAG

Approval Date: February 2016

Date Ratified by Executive Directors: 7th March 2016

Executive Director Lead: Medical Director

Circulation

Issue Date: 9th March 2016

Circulated by: Performance and Information

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? YES

Review

Review Date: November 2017

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 9th March 2016

Contents

1. Introduction and Aims

1.1. The purpose of this Policy is to provide guidance to all Pennine Care NHS Foundation Trust (henceforth referred to as 'the Trust') employees on Data Protection.

1.2. The Trust has a statutory duty to safeguard the information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with the Trust shall misuse any information or allow others to do so.

1.3. During the course of their day to day work, many individuals working within or for the Trust will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period they work for or provide services to the Trust nor at any time after its termination, disclose confidential information that is held or processed by the Trust.

1.4. All staff working for or on behalf of the Trust are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 1998, The Common Law Duty of Confidentiality and, for health and other professionals, through their own professional Codes of Conduct.

1.5. The Trust understands the need for the strictest confidentiality in respect of data. This applies to manual and computer records and conversations about service users' treatments. Everyone working for or on behalf of the Trust is under a legal and common law duty to keep service users' information, held in whatever form, confidential.

1.6. The Information Commissioners Office (ICO) can impose penalties upon the Trust, and/or its employees if non-compliance occurs.

1.7. Confidentiality can only be overridden in exceptional circumstances and with the appropriate justification and be fully documented.

1.8. The Trust will ensure that all personal patient/client/service user (hereafter referred to as 'Service User') and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- Understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the Trust handles information; and
- understand their rights to access information held about them.

1.9. It is the policy of the Trust that all processing of personal information by or on behalf of the Trust, whether as a Data Controller or as a Data Processor for others, shall be in accordance with the requirements of:

- The Data Protection Act (DPA) 1998 and any subsequent amendments

and statutory instruments;
- the current Data Protection registration;
- Trust Policies and Procedures in relation to the protection and use of personal information;
- the Access to Health Records Act 1990 and any subsequent amendments and statutory instruments.

1.10. The aims of this policy are:

- To safeguard all confidential information within the Trust;
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to Data Protection across the Trust;
- to ensure all staff are aware of their responsibilities with regards to confidential information;
- to provide all individuals working within the Trust access to the documents which set out the laws, codes of practice and procedures relating to Data Protection and confidentiality and which apply to them.

1.11 This policy forms part of the overarching Information Governance Framework and Information Governance Policy and related procedure suite.

Information Governance allows organisations and individuals to ensure that information is handled legally, securely, efficiently and effectively. It covers personal confidential information (also commonly known as Personal Confidential Data (PCD)). This is information relating to service users and employees, and corporate information for example financial and People Services.

All parts of the NHS need to establish working practices that effectively deliver the data protection and confidentiality that is required by law, ethics and policy. The objective must be continuous improvement and the NHS is provided with support to deliver changes through the:

- Information Governance Toolkit which will manage and maintain up-to-date policy and guidance and, more generally
- Information Governance teams within the Department of Health
- Cabinet Office Data Handling Review
- Caldicott Review 2 Legislation requires certain safeguards around the confidentiality and disclosure of individual's health information.

2. Scope

2.1. This policy applies to those members of staff that are directly employed by the Trust and for whom the Trust has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the Trust. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the Trust.

2.2. For the purposes of this policy, all information that can be deemed as Personal

Confidential Data (PCD) - that is to say any information which by itself or when put together with another source of information can be used to identify any individual, is included.

2.3. This is irrespective of whether the material is marked as confidential or not.

3. Data Protection Act

3.1. The Data Protection Act 1998 (DPA) governs how we collect, store, process and share data. The Act dictates that information should only be disclosed on a need to know basis. The DPA is an Act of Parliament which defines UK law on the processing of data on identifiable living people.

3.2. The DPA first came into force on March 1st 2000 and covers all personal data held both manually (e.g. on paper, post it note, diaries etc.) and electronically (e.g. on a computer, memory pen, disc, X-ray etc.).

3.3. The DPA is closely linked to the Freedom of Information and Human Rights Acts. Its intention is to focus on promoting the rights of individuals in respect of their privacy and the right to confidentiality of their data.

3.4. Although the Act itself does not mention privacy, it was enacted to bring UK law into line with the EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms, and in particular their right to privacy with respect to the processing of personal data. Anyone holding personal data for any purpose is legally obliged to comply with this Act.

3.5. The Trust is registered with the ICO as a data controller. A data controller must comply with the eight principles of the Data Protection Act (please refer to section 4 of this policy). The Trust Information Governance Lead is the Data Protection Officer. The Trust is committed to compliance with the requirements of the Data Protection Act 1998 and will ensure that all employees and anyone providing a service on behalf of the Trust (directly employed, volunteers and contractors) who have access to any personal data held by or behalf of the Trust, are fully aware of and abide by their duties and responsibilities of the Act.

3.6. The Trust may be required by law to collect and use information about people with whom it works, including service users, members of the public, employees, customers, volunteers and suppliers. This personal information must be handled and managed appropriately however it is collected, recorded and used and whether it is a manual or electronic record.

3.7. The Data Protection Act defines eight data protection principles.

4. Data Protection Principles

4.1. **Data Protection Principle 1 - Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.**

4.1.1 The Trust should only process information where there is an established

legitimate basis to do so. Also it is a requirement to make the general public aware of why the NHS needs information about them, how it will be used and whom it may be disclosed to. The Trust is obliged under the DPA and Caldicott to produce a Privacy Notice. In order to meet the requirements of the first principle a clear consent process is also needed. The Trust Privacy Notice is available via the Information Governance Team, or by following this link: https://www.penninecare.nhs.uk/media/2119/4144-how-we-use-your-information.pdf

4.2. **Data Protection Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

4.2.1. Only use personal information obtained by the Trust in connection with the purpose it was collated.

4.3. **Data Protection Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

4.3.1. Only obtain the minimum amount of information and do not obtain information which is not needed.

4.4. **Data Protection Principle 4 - Personal data shall be accurate and, where necessary kept up to date.**

4.4.1. Ensure that all information entered either manually or electronically is accurate, and where recorded elsewhere ensure that there are appropriate procedures in place to continually review and update the different sources, to ensure accuracy and version control. Where possible do not hold duplicate copies as this increases the risk of inaccurate information being held.

4.5. **Data Protection Principle 5 - Personal data processed for any purpose or purposes shall not be kept longer than necessary for that purpose or those purposes.**

4.5.1. All records are affected by this principle regardless of the media within which they are held/stored and comprehensive guidance is available in the Trusts Records Management Policy**.** When disposing of personal information use only the confidential waste destruction process.

4.6. **Data Protection Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.**

4.6.1. Under this principle of the DPA individuals have the following rights:

- Right of Subject Access;
- right to prevent processing likely to cause harm or distress;
- right to prevent processing for the purposes of direct marketing;
- right in relation to automated decision taking;

- right to take action for compensation if the individual suffers damage;
- right to take action to rectify, block or erase inaccurate data
- right to request an assessment from the Information; Commissioner to establish compliance with the DPA.

4.7. **Data Protection Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

4.7.1. Examples of which are:

- Do not allow unauthorised access;
- do not share passwords and ensure you lock your PC screen before moving away;
- do not leave confidential information on your desk/fax or post trays and ensure all paperwork is tidied away when not in use or at the end of the day.
- PCD should only be shared where appropriate encryption tools are in place.
- The Trust has a suite of policies to fulfil the requirements of Principle 7.

4.8. **Data Protection Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

4.8.1. Countries outside of the EEA do not have the necessary legalisation in place to adequately protect the data covered by the DPA.

5. Personal, Confidential and Sensitive Information

5.1. Personal data is any data which relates to a living individual who can be identified by that data or from that data in conjunction with other information which the data controller is in, or is likely to come into possession of. This includes ‘opinions’ as documented.

5.2. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, personnel records etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

5.3. Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.

5.4. Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified

purposes.

5.5. Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

5.6. Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information (as defined by the Data Protection Act 1998 - DPA) regarding race, health, sexuality, etc.

5.7. Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

5.8. Sensitive data under the terms of the DPA includes but is not restricted to:

- information about a person's racial or ethnic origin;
- political opinions;
- gender;
- religion and belief;
- membership of a trade union;
- Health and sexual life;
- criminal convictions or charges.

This Policy should be read in conjunction with the Trust Confidentiality policy and Information Governance Handbook.

5.9 CALDICOTT PRINCIPLES

5.9.1 In relation to confidentiality, in 1997 Dame Fiona Caldicott delivered a report which made recommendations in order to improve the confidentiality and security of information in the NHS. This introduced 6 principles (below) and the committee produced 18 standards for health organisations to work towards.

5.9.2 For each data flow and use of confidential information, consider the following general principles for using individual-identifiable information:

Principle 1 - Justify the purpose(s)

Principle 2 - Don't use individual-identifiable information unless it is absolutely necessary.

Principle 3 - Use the minimum necessary individual-identifiable information

Principle 4 - Access to individual-identifiable information should be on a strict need to know basis.

Principle 5 - Everyone should be aware of their responsibilities.

Principle 6 - Understand and comply with the law.

5.9.3 In 2013 there was a review of the Caldicott framework as a result of the Caldicott 2 report. This outlined 18 new principles for the NHS regarding protecting patient's confidential data and also introduced a seventh principle which is:

Principle 7 - **The duty to share information can be as important as the duty to protect patient confidentiality.**

Further guidance on the above rules can be found in the guidance document at: http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

6. Roles, Responsibilities and Accountabilities

6.1. Chief Executive (CE)

6.1.1. Although it is the Trust that is the data controller, the CE has overall accountability for compliance with the Data Protection Act (DPA). The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian/SIRO and designated Data Protection Officer. The CE shall ensure that the Trust resubmits an annual data protection notification and fee to the Information Commissioners Office.

6.2. Caldicott Guardian

6.2.1. The Caldicott Guardian will act as the conscience of the Trust, and oversee all disclosures of patient information with particular attention being paid to extraordinary disclosures.

6.3. Senior Information Risk Owner (SIRO)

6.3.1 The SIRO, under delegated authority from the CE will oversee compliance with the DPA and the development of appropriate policy and procedure. The SIRO will be advised by the nominated Data Protection Officer and supported by the Trust Information Governance Officers. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk

6.4 Data Protection Officer (DPO)

6.4.1. The DPO will:

- Ensure the Data Protection Act notification is reviewed, maintained and renewed annually*;*
- ensure that an appropriate Data Protection Policy for the Trust is produced and maintained;
- ensure that the appropriate procedures and practices are formulated and adopted by the Trust;
- represent the Trust on Data Protection matters;
- act as a central point of contact on Data Protection within the Trust;
- provide the appropriate leadership and direction for the Governance team within the Trust;
- ensure all actual or suspected breaches of the Data Protection Act/ confidentiality are managed according to national procedures, monitored and are reported to the appropriate group/committee;

- ensure lawful and timely processing of Subject Access Requests (SAR) in accordance with the requirements of the DPA;
- report performance monitoring data on the handling of SARS received and processed including compliance with turnaround times;
- facilitate appropriate and effective training to Trust staff when required;
- carry out compliance checks;
- maintain an Information Asset Register.

6.4.2 The Data Protection Officer function for the Trust will be performed by the Trust Information Governance Manager, supported by the Information Governance Department.

6.5. Information Asset Owners (IAOs)/Administrators (IAAs)

6.5.1. Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
- will ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- will be responsible for the Information Asset assigned to them;
- will ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a SAR;
- will ensure that personal data held in the Information Asset is maintained in line with the Trusts Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

6.6. Line Managers

- All line managers have a responsibility to ensure that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Protection;
- where a breach of policy/procedure or near miss occurs, line managers will need to comply with the Trust Incident Management processes;

6.7. All Staff and those providing a service on behalf of the service (refers to all trust employees including volunteers/contractor, Agency and Bank/temporary staff and work place students):

- Should adhere to this policy and all related Information Assets and processes to ensure compliance with the DPA;
- are subject to Data Protection compliance and accountable via personal liability;
- have a responsibility to inform the Data Protection Officer of any new

use of personal data immediately;
- must maintain an appropriate level of awareness of the DPA and to complete training as appropriate;
- ensure that all personal information is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset;
- ensure that personal data is not removed from the Trust premises except where specifically required for the execution of legitimate functions of the Trust and, then, only in accordance with appropriate policies;
- ensure that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, microfilm, or any other form, are securely and confidentiality managed and destroyed/erased when they are no longer required for Trust purposes;
- ensure that the Data Protection Officer is advised as soon as possible of any problems or complaints relating to any SAR or unauthorised disclosures/ breaches of confidentiality;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

7. Conduct

7.1. Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by the Trust and/or;
- has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure of an individual and/or;
- has entered the public domain by an authorised disclosure for an unauthorised purpose by the individual or anyone else employed or engaged by the Trust and/or;
- they are required to disclose by law; and/or;
- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regards to the provisions of that Act.

7.2. All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents and/or media, including storage of files on PCs. Confidential information must never be unattended and should be secure when not in use;
- use password protection and not disclose passwords to anyone including work colleagues;
- have regards to the provisions of that Act.

7.3. All individuals will be required to comply with this policy whilst working within the Trust and thereafter for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can no longer be classed as confidential.

7.4. If an individual is unclear if information should be classed as confidential, they must discuss the issue with their line manager who will offer advice.

7.5 **Section 55 offences**.
The Data Protection Section 55 offence makes it an offence (with certain exemptions) to obtain, disclose or procure the disclosure of personal information knowingly or recklessly, without the consent of the organisation holding the information.

Any individual guilty of this offence are punishable by a fine of up to £5,000 in a Magistrates' Court and unlimited in the Crown Court.

8. Subject Access Request

8.1. A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of, personal information that is held about them as an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the Trust, both in electronic and paper files, this is known as a Subject Access Request (SAR).

8.2. Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless of the media which it is held;
- have their information kept up to date;
- require the Trust rectify/block, erase or destroy inaccurate information;
- not have processed confidential information about them likely to cause damage or distress;
- not have processed confidential information about them for the purposes of direct marketing.

8.3. Further information on how the Trust complies with its statutory responsibilities around subject access are available in the Trusts Access to Health Record Policy and SAR Procedure.

9. Disclosing Information

9.1. The Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances the Police. All staff and individuals providing a service on behalf of the Trust should exercise caution when asked to disclose personal data held on another individual to a third party. Where an individual is unsure as to the legitimacy of disclosing information, the Line Manager or a member of the Information Governance Department should always be consulted.

9.2. There may be times when personal data may be legitimately be disclosed, for example where:

- The individual has given their consent for information about them to be disclosed;
- the disclosure is in the legitimate interests of the provision of healthcare (e.g. if members of staff require the information to enable them to perform their jobs adequately or if there are justifiable patient

safety concerns);
- the Trust is legally obliged to disclose the data.

9.3. The NHS Confidentiality: Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.

9.4. Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

9.5. The Trust will inform service users, staff and any other data subjects why, how and for what purpose personal information is collected, recorded and processed. This is known as Fair Processing.

9.6. Consent of the data subject will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

9.7. Under common law, personal information may be disclosed without consent for example:
- In order to prevent serious harm;
- where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

9.8. Where information is required by the police Trust staff should consult the Information Governance Lead.

10. Training and Awareness

10.1. The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA and their IG obligations and this will be carried out by annual mandatory Information Governance training. Any new staff members (including temporary, volunteers and contractors) will be required to complete Information Governance training as part of their induction.

10.2. Information Governance training is required to be undertaken by all employees and those providing a service to the Trust. All NHS staff are mandated to undertake annual Information Governance training.

10.3. Where staff have specific Information Governance roles within the Trust i.e. Caldicott Guardian, SIRO etc. additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the Information Governance Training Plan 2015-18.

10.4. To maintain high staff awareness the Trust will direct staff to a number of sources:
- Policy/strategy and procedure;
- Manuals;

- line manager;
- specific training courses;
- other communication methods, for example, team meetings; bulletins; and the staff Intranet.

11. Disciplinary

11.1. No employee shall knowingly misuse any information or allow others to do so.

11.2. Users must not access records/information that they have no legitimate reason to view, this includes records about themselves their family, friends, neighbours, acquaintances. If there is not a legitimate reason to access information users must not browse and should remember all transactions are auditable.

11.3. If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to the Trust Information Governance Lead.

11.4. Breaches of Data Protection and Confidentiality are a serious matter and will be handled in accordance with the Trust Disciplinary policy and processes.

12. Monitoring and Review

12.1. The Trust will undertake or commission assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

12.2. This policy will be reviewed on a yearly basis, and in accordance with the following on an as and when required basis if the following occurs:

- Legislative changes;
- good practice;
- guidance; case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

12.3. Where there are no significant alterations required, this Policy shall remain for a period of no longer than three years of the ratification date.

13. Relevant Legislation and Related Documents

13.1. Legal Acts:

- Data Protection Act 1998;
- Common Law Duty of Confidentiality
- Human Rights Act;
- Freedom of Information Act 2000;
- Public Interest Disclosure Act 1998;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984 (PACE);
- Copyright, Designs and Patents Act (1988);

- Computer Misuse Act (1990);
- Trademarks Act (1994);
- Terrorism Act (2000);
- Proceeds of Crime Act (2002);
- Money Laundering Regulations (2007);
- Criminal Justice and Immigration Act (2008);
- Environmental Information Regulations;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2006 and 2012 ;
- Human Rights Act 1998.

13.2. Supporting Documents

- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2013 and Caldicott Principles;
- NHS Information Risk Management;
- Records Management Code of Practice (produced under S46 of the Freedom of Information Act 2000);
- The Information Governance Toolkit.
- ICO: Data Sharing Code of Practice

14. Relevant Policies and Procedures

14.1. The following policies and procedures should be read in conjunction with this policy:

- Information Governance Strategy and Policy
- Records Management Policy and Procedure suite
- Information Risk Policy
- Freedom of Information Policy
- Environmental Information Regulations Policy
- I.T and Information Security Policy and Procedure suite
- Confidentiality Guidelines for staff
- IG Staff Handbook
- Trust Fair Processing Notice.